Symantec AntiVirus™ for Network Attached Storage Integration Guide

Symantec AntiVirus™ for Network Attached Storage Integration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.
Documentation version 4.3
PN: 10306135

Copyright Notice

Copyright © 2000-2004 Symantec Corporation.
All Rights Reserved.
Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.
NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.
No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. CarrierScan Server, Bloodhound, LiveUpdate, NAVEX, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation. Sun, Sun Microsystems, the Sun logo, StorEdge, Sun Enterprise, Java, Ultra, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries. Microsoft, ActiveX, Windows, Windows NT, and the Windows Logo are registered trademarks of Microsoft Corporation in the United States and other countries. Red Hat is a registered trademark of Red Hat Software, Inc., in the United States and other countries. Linux is a registered trademark of Linus Torvalds. NetApp, Data ONTAP, NetCache, Network Appliance, and Web Filer are registered trademarks or trademarks of Network Appliance, Inc., in the United States and other countries. Hitachi is a registered trademark of Hitachi, Ltd. Lightning 9900 is a trademark of Hitachi Data Syatems Corporation in the United States and other countries. Adobe, Acrobat, and Acrobat Reader are trademarks of Adobe Systems Incorporated. THIS PRODUCT IS NOT ENDORSED OR SPONSORED BY ADOBE SYSTEMS INCORPORATED, PUBLISHERS OF ADOBE ACROBAT.
Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
A modified version of a freeware SNMP library is used in this software. This software is Copyright © 1988, 1989 by Carnegie Mellon University All Rights Reserved. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.
CMU software disclaimer: “CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.”
A set of Unicode handling libraries is used in this software. This software is Copyright (c) 1995-2002 International Business Machines Corporation and others. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.
IBM software disclaimer: “THE SOFTWARE IS PROVIDED ‘AS IS’, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.”
Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Technical support

Chapter 1 Introducing Symantec AntiVirus™ for Network Attached Storage

About Symantec AntiVirus for Network Attached Storage 11
Supported storage devices 12
Software components 12
How to use the Symantec AntiVirus for Network Attached Storage documentation 12
About the Symantec AntiVirus Scan Engine Implementation Guide 13
About the Symantec AntiVirus for Network Attached Storage Integration Guide 13
Why you need virus protection in a NAS environment 14
How the scan engine protects against viruses 15
About Symantec Security Response 16

Chapter 2 Configuring Symantec AntiVirus for NetApp® Filer™

Software components 17
How the Symantec AntiVirus Scan Engine works with the NetApp Filer client 18
What happens when a file is scanned 18
Connecting to the scan engine 19
Limiting scanning by file type 19
Handling of infected files 20
Logging of scan engine events to the Filer 20
User identification and notification when a virus is found 21
Preparing for installation 21
Configuring the Symantec AntiVirus Scan Engine 22
Configuring RPC 22
Notifying requesting users that a virus was found 26
Quarantining unrepairable infected files 26
Editing the service startup properties 28
Specifying which embedded files to scan 28

Configuring the client NetApp Filer 31
Verifying that the scan engine is registered with the Filer 31
Activating virus scanning 32
Specifying the file extensions to be scanned on the NetApp Filer 32
Known issues with the NetApp Filer 32

Chapter 3 Configuring Symantec AntiVirus for Hitachi® Lightning NAS Blade

Software components 35
How the Symantec AntiVirus Scan Engine works with the Hitachi Lightning NAS Blade 36
How files are scanned 36
How caching works 37
Specifying which file types are scanned 37
Specifying the scan policy 38
Handling of infected files on the Hitachi Lightning NAS Blade 38
Preparing for installation 39
Configuring the Symantec AntiVirus Scan Engine 39
Configuring ICAP-specific options 39
Specifying which file types to scan on the scan engine 41
Scheduling LiveUpdate to update virus definitions automatically 44
Configuring the Hitachi Lightning NAS Blade 45
Registering the Symantec AntiVirus Scan Engine 45
Configuring virus scanning on the Hitachi Lightning NAS Blade 46
Known issues with the Hitachi Lightning NAS Blade 48

Chapter 4 Configuring Symantec AntiVirus for Sun® StorEdge™ 9900 NAS Blade

Software components 52
How the Symantec AntiVirus Scan Engine works with the Sun StorEdge 9900 NAS Blade 52
How files are scanned 52
How caching works 53
Specifying which file types are scanned 53
Specifying the scan policy 54
Handling of infected files on the NAS device 55
Preparing for installation 55
Configuring the Symantec AntiVirus Scan Engine 55
Configuring ICAP-specific options 55
Specifying which file types to scan on the scan engine 58
Scheduling LiveUpdate to update virus definitions automatically 60

Configuring the Sun StorEdge 9900 NAS Blade 61
Registering the Symantec AntiVirus Scan Engine 61
Configuring virus scanning on the Sun StorEdge 9900 NAS Blade 62
Known issues with the Sun StorEdge 9900 NAS Blade 65

Index

Chapter 1

Introducing Symantec AntiVirus™ for Network Attached Storage

This chapter includes the following topics:

- About Symantec AntiVirus for Network Attached Storage
- How to use the Symantec AntiVirus for Network Attached Storage documentation
- Why you need virus protection in a NAS environment

About Symantec AntiVirus for Network Attached Storage

Symantec AntiVirus™ for Network Attached Storage provides virus scanning and repair services for a number of network-attached storage (NAS) devices. You can scan files for viruses automatically as they are accessed from storage before they are accessed by the requesting user. When a virus is found in a file and the file is repaired, the clean file is stored on the NAS device, and the requesting user is granted access.

Supported storage devices

Symantec AntiVirus for Network Attached Storage supports the following storage devices:

- Network Appliance™ (NetApp) Filer™
- Hitachi® Lightning NAS Blade (9900V™ series)
- Sun® StorEdge™ 9900 NAS Blade

Software components

In most cases, adding virus scanning to a supported NAS device requires installation and configuration of the following components:

- The Symantec AntiVirus Scan Engine, which provides the virus scanning and repair services
  The Symantec AntiVirus Scan Engine is included in the Symantec AntiVirus for Network Attached Storage distribution package.
- Connector code that lets the NAS device communicate with the Symantec AntiVirus Scan Engine
  The connector code handles the communication between the scan engine and the NAS device and interprets the results that are returned from the scan engine after scanning. In most cases, the connector code is developed by the manufacturer of the NAS device. The connector code typically is installed and configured on the NAS device. (The connector code may be preinstalled by the manufacturer.)
  In some cases, no connector code is necessary. Communication with the scan engine is handled by the NAS device, and any configuration options are available directly on the device.

How to use the Symantec AntiVirus for Network Attached Storage documentation

To configure Symantec AntiVirus for Network Attached Storage to work with one of the supported NAS devices, you need the documentation that is included in the Symantec AntiVirus for Network Attached Storage distribution package and the documentation that is provided by the manufacturer of the NAS device.

The Symantec AntiVirus for Network Attached Storage distribution package includes the following documents:

- *Symantec AntiVirus Scan Engine Implementation Guide*
- *Symantec AntiVirus for Network Attached Storage Integration Guide*

Because the manufacturer of the NAS device develops the connector code to integrate the Symantec AntiVirus Scan Engine, the manufacturer of the NAS device also prepares and distributes supporting documentation for the connector code. You must obtain the connector code and any supporting documentation from the manufacturer if it does not ship directly with the NAS device.

About the Symantec AntiVirus Scan Engine Implementation Guide

Use the *Symantec AntiVirus Scan Engine Implementation Guide* as the primary guide for installing and configuring the Symantec AntiVirus Scan Engine. This guide contains information that you need to consider about all of the scan engine configuration options.

You will also need to reference the *Symantec AntiVirus for Network Attached Storage Integration Guide* for instructions on configuring the scan engine to work with a specific NAS device.

About the Symantec AntiVirus for Network Attached Storage Integration Guide

The *Symantec AntiVirus for Network Attached Storage Integration Guide* includes a chapter for each supported NAS device. Use the guidance and recommendations that are in the appropriate chapter of this guide, in conjunction with the manufacturer-prepared documentation, to implement virus scanning.

Each chapter in the *Symantec AntiVirus for Network Attached Storage Integration Guide* includes the following information:

- General information on how antivirus scanning works in conjunction with the NAS device

  Virus scanning functionality (for example, handling of infected files, timing of file scanning, logging of infections found) can differ depending on the capabilities of the NAS device and the complexity of the connector code. This section provides an overview of how the Symantec AntiVirus Scan Engine and the NAS device interact during virus scanning.

- Information for configuring the scan engine to work with the NAS device
  This section discusses the configuration options on the scan engine that must be configured to work with the NAS device and may highlight other options that are important in setting up comprehensive virus protection. This information does not replace the *Symantec AntiVirus Scan Engine Implementation Guide*. Consult the implementation guide for installation information and for additional information on configuring the Symantec AntiVirus Scan Engine to meet your needs.
- Information on configuring the NAS device to work with the scan engine
  This section discusses any configuration options on the NAS device that must be configured to work with the Symantec AntiVirus Scan Engine and may make recommendations for configuring the NAS device to ensure comprehensive virus protection. This information does not replace the documentation that is provided by the manufacturer of the NAS device. Consult the product documentation for additional information on configuring the NAS device for virus scanning.
- Known issues
  This section describes issues that can affect operation between the Symantec AntiVirus Scan Engine and the NAS device.

Why you need virus protection in a NAS environment

Network-attached storage provides many benefits, such as increased performance, heterogeneous data access, data redundancy, ease of storage management, and real-time backup recovery. However, the implementation of a NAS system introduces security risks that should be addressed. When data is consolidated into a centralized NAS system, which is typically connected directly to the local network, data can be accessed and compromised much more quickly.

Installing virus protection software at key locations in the corporate network, for example, firewalls, email gateways, and desktops is not sufficient to protect data on NAS servers.

Dedicated antivirus protection for a NAS system should be part of a comprehensive security policy for the following reasons:

- Storage servers, because they are accessed by large numbers of users and contain large amounts of data, are susceptible to attack from viruses, worms, Trojan horses, and other malicious code.

- Malicious code can result in lost, stolen, or corrupted files, which can result in costly downtime to the enterprise.
- Once a threat is stored on the NAS system, the NAS system can become a vector for the malicious code, which can comprome the computers and the data of the users who access the NAS system.
- Through NAS backup, mirroring of data, and archiving, malicious code can be replicated multiple times in multiple locations. When NAS data that contains malicious code is restored from one of these locations, the malicious code can be reintroduced to the NAS system, thereby potentially reinfecting the network.
- With the possibility of malicious code being replicated on the NAS system in multiple locations and infecting other parts of the network, the effort to effectively remove a threat becomes an overwhelming task that involves significant downtime as well as time and money for data recovery.
- The NAS system can be used as an access point to the rest of the network or as a launch point for an attack (for example, a denial of service attack).
- Industry regulations and laws now require organizations that maintain financial, medical, personal, and email data to protect that data from being stolen, altered, or destroyed. Organizations are legally responsible for providing comprehensive protection for stored data.

How the scan engine protects against viruses

The Symantec AntiVirus Scan Engine detects viruses, worms, and Trojan horses in all major file types (for example, Windows files, DOS files, and Microsoft Word and Excel files). The Symantec AntiVirus Scan Engine includes a decomposer that handles most compressed and archive file formats and nested levels of files. You can configure the scan engine to limit scanning to certain file types based on file extension.

The Symantec AntiVirus Scan Engine provides protection against container files that can cause denial of service attacks (for example, container files that are overly large, that contain large numbers of embedded compressed files, or that have been designed to use resources maliciously and degrade performance). You can specify the maximum amount of time that the scan engine devotes to decomposing a file and its contents, the maximum file size for container files, and the maximum number of nested levels to be decomposed for scanning.

The Symantec AntiVirus Scan Engine also detects mobile code such as Java™, ActiveX®, and stand-alone script-based threats. The Symantec AntiVirus Scan Engine uses Symantec antivirus technologies, including Bloodhound™, for heuristic detection of new or unknown viruses; NAVEX™, which provides protection from new classes of viruses automatically through LiveUpdate; and Striker, for the detection of polymorphic viruses.

About Symantec Security Response

The Symantec AntiVirus Scan Engine is supported by the Symantec Security Response team. These Symantec engineers work 24 hours per day, 7 days per week, tracking new virus outbreaks and identifying new virus threats.

For more information about protection against a specific virus, visit the Symantec Security Response Web site at:

http://securityresponse.symantec.com

For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Chapter 2

Configuring Symantec AntiVirus for NetApp® Filer™

This chapter includes the following topics:

- Software components
- How the Symantec AntiVirus Scan Engine works with the NetApp Filer client
- Preparing for installation
- Configuring the Symantec AntiVirus Scan Engine
- Configuring the client NetApp Filer
- Known issues with the NetApp Filer

Software components

Symantec AntiVirus for Network Attached Storage provides virus scanning and repair capabilities for Network Appliance™ (NetApp) Filer™ storage appliances.

To add antivirus scanning to the NetApp Filer, you must configure the following components:

- The Symantec AntiVirus Scan Engine, which provides the virus scanning and repair services
  For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

- The NetApp Filer
  Some options are configured directly on the NetApp Filer. No additional code is necessary to connect the Symantec AntiVirus Scan Engine to the NetApp Filer.

How the Symantec AntiVirus Scan Engine works with the NetApp Filer client

Symantec AntiVirus for Network Attached Storage provides virus scanning and repair capabilities for NetApp Filer storage appliances that support Data ONTAP™ version 6.1.3R2 or later. If you plan to use a single Symantec AntiVirus Scan Engine to support multiple Filer storage appliances, each Filer must be running Data ONTAP 6.3.1 or later.

The Symantec AntiVirus Scan Engine must be installed on a computer that is running Windows 2000 Server/Server 2003. It must be located in the same domain as the NetApp Filer for which it will provide scanning and repair services. The Symantec AntiVirus Scan Engine uses the proprietary Network Appliance adaptation of the RPC protocol to interface with NetApp Filer storage appliances.

A single Symantec AntiVirus Scan Engine can support multiple NetApp Filers. For sites with larger scan volumes, you can use multiple scan engines to support one or more Filers. Load balancing is handled through the NetApp Filer interface.

Virus scanning on the NetApp Filer is available only for files that are requested through the Common Internet File System (CIFS). Files that are requested through the Network File System (NFS) are not scanned for viruses.

What happens when a file is scanned

The NetApp Filer submits files to the Symantec AntiVirus Scan Engine for scanning on both read and write. That is, files are scanned when they are submitted for storage or changed on the Filer (write) or when they are accessed from storage (read).

When a user attempts to access a file, the Filer passes the file to the Symantec AntiVirus Scan Engine for scanning. After a file is scanned, the Symantec AntiVirus Scan Engine indicates the scanning results to the Filer. If a file is infected and can be repaired, the scan engine returns the repaired file.

After the Filer receives the scanning results, clean files are passed to the requesting user. If the file is infected and can be repaired, the repaired file is passed to the requesting user, and the stored version of the infected file is

replaced with the repaired file. If the file is infected and cannot be repaired, the user is denied access to the file, and the infected file is deleted from storage.

The Filer caches scanning results for each clean file to avoid redundant scans of files that have already been scanned. The cache is purged when the virus definitions on the Symantec AntiVirus Scan Engine are updated or the scan engine is restarted. If the cache is full and a file that is not in the cache is accessed, the oldest information in the cache is purged so that the scanning results for the newly scanned file can be stored.

Connecting to the scan engine

A connection is maintained between each NetApp Filer and the Symantec AntiVirus Scan Engine. The Symantec AntiVirus Scan Engine monitors the connection with each NetApp Filer by checking the connection at a configured time interval. If the scan engine determines that the connection is not active, it tries to reconnect. (The number of times that the scan engine tries to reestablish the connection can also be configured.) If the Symantec AntiVirus Scan Engine makes the maximum number of tries with no reply from any NetApp Filer, the Symantec AntiVirus Scan Engine shuts down.

Limiting scanning by file type

Viruses are found only in file types that contain executable code. Because it is not necessary to scan every file type, you can save bandwidth and time by limiting the files to be scanned to only those file types that can contain viruses.

You have the following levels of control over which files are scanned:

- You can control the files that are initially submitted to the scan engine by the NetApp Filer for scanning.

  The NetApp Filer lets you specify by file extension which files are passed to the Symantec AntiVirus Scan Engine for scanning. You configure the file types that you want to submit for scanning through the NetApp Filer interface in accordance with the product documentation.

- You can control which files of those that are embedded in archival file formats (for example, .zip or .lzh files) are scanned by the Symantec AntiVirus Scan Engine.
  The scan engine lets you specify extensions that you do not want to scan (using an exclusion list) or specify extensions that you want to scan (using an inclusion list). You can also scan all file types regardless of extension. You configure which embedded files are scanned through the Symantec AntiVirus Scan Engine administrative interface.
  See "Specifying the file extensions to be scanned on the NetApp Filer" on page 32.

Handling of infected files

You can configure the Symantec AntiVirus Scan Engine to do any of the following when an infected file is found:

- Scan only: Deny access to the infected file, but do nothing to the infected file.
- Scan and repair files: Attempt to repair the infected file, and deny access to any unrepairable file.
- Scan and repair or delete: Attempt to repair the infected file, and delete any unrepairable file.

Unrepairable files also can be quarantined.

See"Quarantining unrepairable infected files" on page 26.

Logging of scan engine events to the Filer

Certain Symantec AntiVirus Scan Engine events are logged automatically to the Filer's logging subsystem. Logging to the Filer is not affected by the logging options you can activate in the Symantec AntiVirus Scan Engine.

The following scan engine events are logged to the Filer:

- Unrepairable infections
- Container violations
- Scans that are aborted because the antivirus scanning license is expired
- Unrepairable files that are sent to the quarantine server
- Failed attempts to send unrepairable files to the quarantine server

User identification and notification when a virus is found

When a virus is found in a file that is requested from the NetApp Filer, the Symantec AntiVirus Scan Engine automatically obtains (for logging purposes) identification information about the user who requested the infected file. This information includes the security identifier of the user and the IP address and host name of the requesting computer.

The identification information supplements the information that is contained in Infection Found log messages that are logged to the local logs, the Windows Event Log, and SMTP. However, this information does not appear in Infection Found messages that are logged to SNMP or SESA.

Note: The Symantec AntiVirus Scan Engine can obtain only the information that is made available by the NetApp Filer. In some cases, all or some of this information is not available. The information that is obtained is reported in the related log entries. Any identification information that is not obtained from the NetApp Filer is omitted from the log messages and from the user notification window.

You also can configure the Symantec AntiVirus Scan Engine to notify the requesting user that the retrieval of a file failed because a virus was found. The notification message only displays if the user is using a Windows computer. The notification message includes the date and time of the event, the file name of the infected file, the virus name and ID, the virus definition date and revision number, and the manner in which the infected file was handled (for example, the file was repaired or deleted).

To use the user notification feature, the Windows Messenger service must be running on the computer that is running the Symantec AntiVirus Scan Engine, as well as the user's computer.

See "Notifying requesting users that a virus was found" on page 26.

Preparing for installation

To interface with the Symantec AntiVirus Scan Engine, the Network Appliance Filer storage appliance must support Data ONTAP version 6.1.3R2 or later. If you plan to use a single Symantec AntiVirus Scan Engine to support multiple Filer storage appliances, each Filer must support Data ONTAP 6.3.1 or later. Before you install the scan engine, ensure that each NetApp Filer for which the scan engine is to provide scanning and repair services meets this requirement.

To use RPC, the Symantec AntiVirus Scan Engine must be installed on a computer that is running Windows 2000 Server/Server 2003. Ensure that the

computer on which you plan to install the Symantec AntiVirus Scan Engine meets the system requirements that are listed in the *Symantec AntiVirus Scan Engine Implementation Guide*.

After you have installed the Symantec AntiVirus Scan Engine, you must configure the NetApp Filer to work with the scan engine.

See "Configuring the client NetApp Filer" on page 31.

Configuring the Symantec AntiVirus Scan Engine

The Symantec AntiVirus Scan Engine must be configured to use RPC as the communication protocol. The Internet Content Adaptation Protocol (ICAP) is the default protocol at installation, so you must change the protocol to RPC through the administrative interface. After you have selected RPC, you must configure several RPC-specific options.

You must also change the Windows service startup properties to identify an account that has the appropriate permissions.

See "Editing the service startup properties" on page 28.

Configuring RPC

After you install the Symantec AntiVirus Scan Engine, you can configure several settings that are specific to the RPC protocol. When you change to the RPC protocol through the Symantec AntiVirus Scan Engine administrative interface, you must manually stop and restart the scan engine service (rather than clicking Restart on the administrative interface) to properly connect to the NetApp Filer.

Table 2-1 describes the protocol-specific options for RPC.

Table 2-1 Protocol-specific options for RPC

Option	Description
RPC client IP addresses	A single Symantec AntiVirus Scan Engine can support one or more NetApp Filers. NetApp Filers must be located in the same domain as the scan engine. You must provide the IP address of each NetApp Filer. **Note:** Multiple scan engines can support a single NetApp Filer. Configuration for multiple scan engines is configured through the NetApp Filer interface.

Table 2-1 Protocol-specific options for RPC

Option	Description
Check RPC connection every __ seconds	The Symantec AntiVirus Scan Engine maintains a connection with the NetApp Filer. The Symantec AntiVirus Scan Engine can be configured to check the connection with the NetApp Filer at a prescribed interval to ensure that the connection is active. The default value is 20 seconds.
Maximum number of reconnect attempts	You can configure the scan engine to make a specified number of attempts to reestablish a lost connection with the NetApp Filer. If the maximum number of attempts is exceeded with no reply from the NetApp Filer, the Symantec AntiVirus Scan Engine shuts down. By default, the Symantec AntiVirus Scan Engine is configured to try to reconnect with the NetApp Filer indefinitely. **Note:** Do not set a maximum number of reconnect attempts if the scan engine is providing scanning for multiple NetApp Filers. Use the default setting.
RPC scan policy	You can configure the Symantec AntiVirus Scan Engine to do one of the following when an infected file is found: ■ Scan only: Deny access to the infected file, but do nothing to the infected file. ■ Scan and repair files: Attempt to repair the infected file, and deny access to any unrepairable file. ■ Scan and repair or delete: Attempt to repair the infected file, and delete any unrepairable file. **Note:** If you plan to quarantine infected files that cannot be repaired, you must select Scan and repair or delete. For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.
Quarantine unrepairable files	You can quarantine unrepairable infected files using Symantec Central Quarantine. Symantec Central Quarantine is included on the Symantec AntiVirus Scan Engine distribution CD along with supporting documentation. For more information, see "Quarantining unrepairable infected files" on page 26. Also see the Symantec Central Quarantine document (CentQuar.pdf), which is included on the CD.

Configure RPC

To configure RPC, you must do the following:

- Provide an IP address for each NetApp Filer for which the Symantec AntiVirus Scan Engine will provide scanning services. You can add or delete Filers from this list at any time.

- Configure the additional RPC-specific options.

To edit the list of NetApp Filers

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **RPC**.
   The configuration settings are displayed for the selected protocol.
3. To add a NetApp Filer to the list of RPC clients, do the following:
   - In the IP address box, type the IP address of the NetApp Filer for which the Symantec AntiVirus Scan Engine will provide scanning services.
   - Click **Add**.
     The list of NetApp Filers updates to reflect your changes.
4. To delete a NetApp Filer from the list of RPC clients, do the following:
   - In the list of RPC clients, select the IP address of the NetApp Filer that you want to delete.
     You can select more than one entry by either holding down Shift and selecting the first and last entries to be deleted (all entries in between will be highlighted), or by holding down CTRL and selecting the individual entries to be deleted.
   - Click **Delete**.
5. Click **Confirm Changes** to save the configuration.
6. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the scan engine service now.
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

To configure additional RPC-specific options

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **RPC**.
   The configuration settings are displayed for the selected protocol.
   If you change to or from the RPC protocol through the Symantec AntiVirus Scan Engine administrative interface, you must manually stop and restart the service (rather than clicking Restart on the administrative interface) to properly connect to or disconnect from the NetApp Filer.
3. In the Check RPC connection every box, type how frequently the Symantec AntiVirus Scan Engine checks the RPC connection with the NetApp Filer to ensure that the connection is active.
   The default interval is 20 seconds.
4. In the Maximum number of reconnect attempts box, type the maximum number of attempts that the Symantec AntiVirus Scan Engine will make to reestablish a lost connection with the NetApp Filer.
   The default setting is 0, which causes the Symantec AntiVirus Scan Engine to try indefinitely to reestablish a connection. Use the default setting if the scan engine is providing scanning for multiple NetApp Filers.
5. In the RPC scan policy list, select how you want the Symantec AntiVirus Scan Engine to handle infected files.
   The default setting is Scan and repair or delete.
6. Click **Confirm Changes** to save the configuration.
7. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

   Do not click Restart. The Symantec AntiVirus Scan Engine will not connect or disconnect from the NetApp Filer properly if you click Restart on the administrative interface.
8. Stop and restart the Symantec AntiVirus Scan Engine service manually.
   You must stop and restart the service manually if you have changed to or from RPC using the administrative interface (rather than selecting the protocol during installation).

Notifying requesting users that a virus was found

You can configure the Symantec AntiVirus Scan Engine to notify the requesting user that the retrieval of a file failed because a virus was found. The notification message only displays if the user is using a Windows computer.

The notification message includes the following:

- The date and time of the event
- The file name of the infected file
- The virus name and ID
- The manner in which the infected file was handled (for example, the file was repaired or deleted)

To notify requesting users that a virus was found

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Logging tab, under Log Windows Messenger, check **Enable Windows Messenger Logging**.
   User notification is disabled by default.
3. Click **Confirm Changes** to save the configuration.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the scan engine service now.
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

Quarantining unrepairable infected files

When you are using the RPC protocol, you can quarantine unrepairable infected files. Symantec Central Quarantine must be installed separately.

The Symantec AntiVirus Scan Engine forwards infected items that cannot be repaired to Symantec Central Quarantine. Typically, heuristically detected viruses that cannot be eliminated by the current set of virus definitions are forwarded to the quarantine and isolated so that the viruses cannot spread. From the quarantine, the infected items can be submitted to Symantec Security

Response for analysis. If a new virus is identified, new virus definitions are posted.

Note: You must select Scan and repair or delete as the RPC scan policy to forward files to the quarantine. Once a copy of an infected file is forwarded to the quarantine, the original infected file is deleted. If submission to the quarantine is not successful, the original file is not deleted, and an error message is returned to the NetApp Filer. In this case, access to the infected file is denied.

For more information about installing and configuring Symantec Central Quarantine, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

To quarantine unrepairable infected files

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, under RPC specific configuration, check **Quarantine unrepairable files**.
3. In the Quarantine Server box, type the host name or the IP address for the computer on which Symantec Central Quarantine is installed.
4. In the Quarantine Port box, type the TCP/IP port number to be used by the Symantec AntiVirus Scan Engine to pass files to Symantec Central Quarantine.
   This setting must match the port number that is selected at installation for Symantec Central Quarantine.
5. Click **Confirm Changes** to save the configuration.
6. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
   - If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the scan engine service now.
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

Editing the service startup properties

If you change the protocol setting to RPC through the Symantec AntiVirus Scan Engine administrative interface, you might need to change the service startup properties to identify an account that has the appropriate permissions. This account must have Backup Operator privileges on the NetApp Filer.

Note: If you select RPC at installation, you are prompted for the account name and password for this account as part of the installation process and do not need to edit the service startup properties manually. This step is necessary only if you change protocols after installation through the administrative interface (rather than uninstalling and reinstalling the scan engine).

To edit the service startup properties

1. In the Windows 2000/2003 Control Panel, click **Administrative Tools**.
2. Click **Services**.
3. In the list of services, right-click **Symantec AntiVirus Scan Engine**, and then click **Properties**.
4. In the Properties dialog box, on the Log On tab, click **This Account**.
5. Type the account name and password for the account on which the Symantec AntiVirus Scan Engine will run.
   Use the following format for the account name:
   domain\username
6. Click **OK**.
7. Stop and restart the Symantec AntiVirus Scan Engine service.

Specifying which embedded files to scan

The NetApp Filer submits files to the Symantec AntiVirus Scan Engine for scanning based on the file extension of the top-level file. The file types that are submitted for scanning are configurable through the Filer administrative interface. Top-level files that are sent to the Symantec AntiVirus Scan Engine are scanned regardless of file extension.

When the scan engine receives an archive file (for example, a .zip or .lzh file) that contains embedded files, it must break down the archive file and scan each embedded file. You can control, through the scan engine administrative interface, which embedded files are scanned by using an exclusion or an inclusion list, or you can scan all files regardless of extension.

The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with extensions that are listed in a prepopulated exclusion list. The default exclusion list contains those file types that are unlikely to contain viruses, but you can edit this list.

Using an inclusion list to control which types of files are scanned is the least secure setting. Only those file types that are listed in an inclusion list are scanned. Thus, with an inclusion list, there is an almost limitless number of possible file extensions that are not scanned. For this reason, the Symantec AntiVirus Scan Engine inclusion list is not prepopulated. However, you can populate this list if you want to limit the file types that are scanned.

Note: During virus outbreaks, you might want to scan all files even if you normally control the file types that are scanned with the inclusion or exclusion list.

Specify which embedded file types to scan

You can scan all files regardless of extension, or you can control which file types are scanned by specifying extensions that you want to include or exclude. The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with extensions that are listed in the prepopulated exclusion list.

To scan all files regardless of extension

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files regardless of extension**.
3. Click **Confirm Changes** to save the configuration.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the scan engine service now.
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

To scan all files except for those with extensions that are in the exclusion list

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files except those with the following extensions**.
3. Edit the exclusion list to add extensions that you do not want to scan or delete extensions that you want to scan.
   Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To exclude files with no extension, use two adjacent semicolons (for example, .com;.exe;;).
4. To restore the default extension list, click **Restore default lists**.
5. Click **Confirm Changes** to save the configuration.
6. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the scan engine service now.
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

To scan only files with extensions that are in the inclusion list

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, check **Scan files with the following extensions**.
3. Edit the inclusion list to add extensions that you want to scan or delete extensions that you do not want to scan.
   The inclusion list is blank by default. Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To scan files that have no extensions, use two adjacent semicolons (for example, .com;.exe;;).
4. Click **Confirm Changes** to save the configuration.

5 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

Configuring the client NetApp Filer

After you have configured the Symantec AntiVirus Scan Engine to use RPC as the communication protocol, you must configure the client NetApp Filers to work with the Symantec AntiVirus Scan Engine.

To interface with the Symantec AntiVirus Scan Engine, NetApp Filer clients must be running Data ONTAP version 6.1.3R2 or later. If you plan to support more than one Filer with a single scan engine, each Filer must be running Data ONTAP 6.3.1 or later.

Each NetApp Filer should be installed and configured in accordance with the accompanying product documentation. Each Filer should be working properly before you initiate virus scanning using the Symantec AntiVirus Scan Engine.

Verifying that the scan engine is registered with the Filer

After you have installed the Symantec AntiVirus Scan Engine, you can verify that the scan engine is registered with the Filer. If you have provided the correct information to the Symantec AntiVirus Scan Engine for contacting the Filer, registration is automatic when the scan engine connects to the Filer. Use the vscan command to check the list of registered scan engines.

Note: If you have not changed the service startup properties for the Symantec AntiVirus Scan Engine to identify an account that has the appropriate permissions on the Filer, the scan engine cannot register with the Filer because it does not have sufficient permission. See “Editing the service startup properties” on page 28.

Activating virus scanning

You can activate and deactivate virus scanning. Use the vscan on command to activate virus scanning. Use the vscan off command to deactivate virus scanning.

Specifying the file extensions to be scanned on the NetApp Filer

To control the file types that are passed to the Symantec AntiVirus Scan Engine for scanning based on file extension, you must configure the list of extensions on the NetApp Filer to contain only the file extensions that you want to scan.

A default list of extensions to be submitted for virus scanning is included with the NetApp Filer. Use the NetApp vscan command to add additional extensions to the extension list on the NetApp Filer.

Using the wildcard extension (???) on the NetApp Filer to have all files scanned regardless of file extension might negatively impact performance. Although scanning all file types provides the highest level of protection, viruses are found only in file types that contain executable code. It is not necessary to scan every file type. You can save bandwidth and time by limiting the files to be scanned to only those file types that can contain viruses.

For more information, see the NetApp Filer documentation.

Known issues with the NetApp Filer

The following are known issues with the NetApp Filer:

- The NetApp Filer might occasionally time out while waiting for a reply from the Symantec AntiVirus Scan Engine when large or complex files are being scanned (for example, container files with multiple embedded files or files that contain polymorphic or macro viruses).

  When a scan request times out, the NetApp Filer submits the request again. If the second request times out, access to the file is denied. Network Appliance plans to provide a fix for this issue in an upcoming release.

- If you have not edited the service startup properties for the Symantec AntiVirus Scan Engine to identify an account with Backup Operator privileges on the NetApp Filer, backups on the Filer might not finish successfully when virus scanning is active.

  The NetApp Filer can time out while waiting for a reply from the Symantec AntiVirus Scan Engine when large files are being scanned. Virus scanning also increases the length of time that is needed for a backup to finish.

  Make sure that you have edited the service startup privileges appropriately, or disable virus scanning before you initiate a backup of the NetApp Filer.

  See "Editing the service startup properties" on page 28.

Chapter 3

Configuring Symantec AntiVirus for Hitachi® Lightning NAS Blade

This chapter includes the following topics:

- Software components
- How the Symantec AntiVirus Scan Engine works with the Hitachi Lightning NAS Blade
- Preparing for installation
- Configuring the Symantec AntiVirus Scan Engine
- Configuring the Hitachi Lightning NAS Blade
- Known issues with the Hitachi Lightning NAS Blade

Software components

Symantec AntiVirus for Network Attached Storage provides virus scanning and repair capabilities for the Hitachi Lightning 9900V™ series of network-attached storage (NAS) devices.

Adding antivirus scanning to the Hitachi Lightning NAS Blade requires configuration of the following components:

- The Symantec AntiVirus Scan Engine, which provides the virus scanning and repair services
  For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

- The NAS Anti Virus Agent
  The NAS Anti Virus Agent provides the virus scanning functionality and must be installed and configured on all Hitachi Lightning NAS Blades in a cluster.

How the Symantec AntiVirus Scan Engine works with the Hitachi Lightning NAS Blade

Symantec AntiVirus for Network Attached Storage provides virus scanning and repair capabilities for the Lightning 9900V series of network-attached storage devices. Virus scanning and repair is provided for files on the Common Internet File System (CIFS).

The Internet Content Adaptation Protocol (ICAP) is used to communicate with the Symantec AntiVirus Scan Engine. In a typical Hitachi NAS environment, a minimum of two scan engines is required to handle scan volume. Four or more scan engines are recommended. The NAS Anti Virus Agent handles load balancing across multiple scan engines automatically.

How files are scanned

You have the following options for controlling when the Hitachi Lightning NAS Blade submits files to the Symantec AntiVirus Scan Engine for scanning:

- Read and write (recommended): Files are scanned when they are submitted for storage or changed on the NAS device (write) or when they are accessed from storage (read).
- Read: Files are scanned on read only.
- Write: Files are scanned on write only.

When a user attempts to access a file from storage, the NAS Anti Virus Agent opens a connection with the Symantec AntiVirus Scan Engine and passes the file to the scan engine for scanning. When scanning is complete, the NAS Anti Virus Agent closes the connection with the scan engine.

After a file is scanned, the Symantec AntiVirus Scan Engine indicates the scanning results to the NAS Anti Virus Agent. If a file is infected and can be repaired, the scan engine also returns the repaired file.

After the NAS Anti Virus Agent receives the scanning results, the file is handled according to the configuration options that are selected. Clean files are passed to the requesting user. If the file is infected and can be repaired, the repaired file is passed to the requesting user, and the stored version of the infected file is

replaced with the repaired file. If the file is infected and cannot be repaired, the user is denied access to the file, and the infected file is deleted from storage.

How caching works

The NAS Anti Virus Agent caches scanning results for each clean file. The cached information includes the date and revision number of the virus definitions that were used to perform the scan. In this way, if a second user requests access to a file that has already been scanned and the virus definitions have not changed, a redundant scan is avoided.

The cache is purged when the virus definitions on the Symantec AntiVirus Scan Engine are updated and when the Hitachi Lightning NAS Blade is restarted. Individual cache entries are updated whenever a stored file is changed.

Specifying which file types are scanned

To specify the types of files to be scanned for viruses, you must configure settings on both the NAS Anti Virus Agent and the Symantec AntiVirus Scan Engine.

Specifying file types on the NAS Anti Virus Agent

The NAS Anti Virus Agent makes an initial determination, based on file extension, about whether to pass a file to the Symantec AntiVirus Scan Engine for scanning. You configure which files are passed to the Symantec AntiVirus Scan Engine for scanning when you set up the NAS Anti Virus Agent.

You can control which files are scanned by using either an exclusion or an inclusion list, or you can scan all files regardless of extension. You should configure the NAS Anti Virus Agent to pass all file types to the scan engine except those that are contained in the exclusion list. The default exclusion list is prepopulated with extensions for those file types that are not likely to contain viruses and can be excluded from scanning. You can customize this list.

See “Configuring virus scanning on the Hitachi Lightning NAS Blade” on page 46.

Specifying file types on the Symantec AntiVirus Scan Engine

The Symantec AntiVirus Scan Engine must be configured to scan selected file types. The scan policy on the Symantec AntiVirus Scan Engine is as important as the NAS Anti Virus Agent setting. It is used after the scan engine receives a file from the NAS Anti Virus Agent to determine which files to scan of those that are contained in archive or container file formats. You can control which

embedded files are scanned by using either an exclusion or an inclusion list, or you can scan all files regardless of extension.

Note: Inclusion and exclusion lists do not scan all file types; therefore, new types of viruses might not be detected. Scanning all files regardless of extension is the most secure setting, but it imposes the heaviest demand on resources. During virus outbreaks, you might want to scan all files even if you normally control the file types that are scanned with the inclusion or exclusion list.

For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

See "Specifying which file types to scan on the scan engine" on page 41.

Specifying the scan policy

You configure the scan policy through the Symantec AntiVirus Scan Engine administrative interface. When an infected file is found, the scan engine can do any of the following:

- Scan only: Scan files for viruses, but do nothing to infected files.
- Scan and delete: Scan files for viruses, and delete any infected files that are embedded in archive or container files without attempting repair.
- Scan and repair files: Attempt to repair infected files, but do nothing to unrepairable files (that is, do not delete the files from archive or container files).
- Scan and repair or delete: Attempt to repair infected files, and delete unrepairable files from archive or container files.

Handling of infected files on the Hitachi Lightning NAS Blade

When an unrepairable infected file is found, the NAS Anti Virus Agent can be configured to do any of the following:

- Delete the file: Deny access to the file, and delete the infected file from storage.
  If the file has not yet been stored on the Hitachi Lightning NAS Blade, the temporary backup copy of the file is deleted and the file is not stored.
- Deny access: Deny access to the file, but do not delete the file from storage.
- Allow access: Allow access to the infected file, and do not delete the file from storage.

Preparing for installation

Ensure that the computer on which you plan to install the Symantec AntiVirus Scan Engine meets the system requirements that are listed in the *Symantec AntiVirus Scan Engine Implementation Guide*.

After you have installed the Symantec AntiVirus Scan Engine, you must configure the virus scanning functionality on the Hitachi Lightning NAS Blade.

Configuring the Symantec AntiVirus Scan Engine

You must configure several settings on each Symantec AntiVirus Scan Engine that is used to support scanning for the Hitachi Lightning NAS Blade.

Warning: If you are using multiple scan engines to support scanning, the configuration settings on each scan engine must be identical. LiveUpdate should be scheduled to occur at the same time on all scan engines so that virus definitions are consistent at all times.

The scan engine must be configured to use ICAP as the communication protocol. ICAP is the default protocol at installation. After you have selected ICAP, you must configure several ICAP-specific options.

Configuring ICAP-specific options

After you install the Symantec AntiVirus Scan Engine, you can configure several settings that are specific to the ICAP protocol through the Symantec AntiVirus Scan Engine administrative interface. If the Symantec AntiVirus Scan Engine has already been configured to use another protocol, you also can change the protocol through the administrative interface.

For more information about accessing the administrative interface, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Table 3-1 describes the protocol-specific options for ICAP.

Table 3-1 Protocol-specific options for ICAP

Option	Description
Scan engine bind address	By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by entering the appropriate bind address.

Table 3-1 Protocol-specific options for ICAP

Option	Description
Port number	The port number must be exclusive to the Symantec AntiVirus Scan Engine. For ICAP, the default port number is 1344. If you change the port number, use a number greater than 1024 that is not in use by any other program or service.
HTML message displayed for infected files	This setting is not applicable for the Hitachi Lightning NAS Blade and should be left at the default setting.
ICAP scan policy	When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following: ■ Scan only: Scan files for viruses, but do nothing to infected files. ■ Scan and delete: Scan files for viruses, and delete any infected files that are embedded in archive or container files without attempting repair. ■ Scan and repair files: Attempt to repair infected files, but do nothing to unrepairable files (that is, do not delete the files from archive or container files). ■ Scan and repair or delete: Attempt to repair infected files, and delete unrepairable files from archive or container files.
Data trickle	This setting is not applicable for the Hitachi Lightning NAS Blade. This setting should be left at the default setting (off).

To configure ICAP-specific options

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.

2 On the Protocol tab, click **ICAP**.
The configuration settings are displayed for the selected protocol.
If you change the protocol setting from RPC to ICAP through the Symantec AntiVirus Scan Engine administrative interface, you must manually stop and restart the service (rather than clicking Restart on the administrative interface).

3 Under ICAP Protocol Configuration, in the Scan Engine bind address box, type a bind address, if necessary.
By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address.

4 In the Port number box, type the TCP/IP port number that the NAS Anti Virus Agent uses to pass files to the Symantec AntiVirus Scan Engine for scanning.
The default setting for ICAP is port 1344.

5 In the ICAP scan policy list, select how you want the Symantec AntiVirus Scan Engine to handle infected files.
The default setting is Scan and repair or delete. This is the recommended setting.

6 Click **Confirm Changes** to save the configuration.

7 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
  You must stop and restart the service manually if you change the communication protocol setting from RPC to ICAP through the administrative interface (rather than selecting ICAP at installation).
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

Specifying which file types to scan on the scan engine

To specify the types of files to be scanned for viruses, you must configure settings on the Symantec AntiVirus Scan Engine. The scan policy on the Symantec AntiVirus Scan Engine is used after the scan engine receives a file from the NAS Anti Virus Agent to determine which files to scan of those that are contained in archive or container file formats.

You can control which embedded files are scanned by using either an exclusion or an inclusion list, or you can scan all files regardless of extension. The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with extensions that are listed in the prepopulated exclusion list.

Note: The Symantec AntiVirus Scan Engine examines the first few bytes of every file to determine whether the file could contain a virus, even if the file extension is not one that was identified for scanning. Based on this examination, the scan engine may scan a file even though it has not been identified for scanning.

For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

See "Configuring virus scanning on the Hitachi Lightning NAS Blade" on page 46.

Specify which file types to scan

You can control which file types are scanned by specifying extensions that you want to include or exclude from scanning, or you can scan all files regardless of extension.

To scan all files except for those that are in the exclusion list

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files except those with the following extensions**.
   This is the recommended setting.
3. Edit the exclusion list to add extensions that you do not want to scan or to delete extensions that you want to scan.
   Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To exclude files with no extension, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.
4. To restore the default extension list, click **Restore default lists**.
5. Click **Confirm Changes** to save the configuration.

6 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

To scan only files that are in the inclusion list

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.

2 On the AntiVirus tab, under File types to be scanned, check **Scan files with the following extensions**.

3 Edit the inclusion list to add extensions that you want to scan or to delete extensions that you do not want to scan.
Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To scan files that have no extensions, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.

4 Click **Confirm Changes** to save the configuration.

5 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

To scan all files regardless of extension

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.

2 On the AntiVirus tab, under File types to be scanned, click **Scan all files regardless of extension**.

3 Click **Confirm Changes** to save the configuration.

4 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

Scheduling LiveUpdate to update virus definitions automatically

Scheduling LiveUpdate to occur automatically at a specified time interval ensures that the Symantec AntiVirus Scan Engine always has the most current virus definitions. If you are using multiple scan engines to support virus scanning, scheduling LiveUpdate to occur at the same time for each scan engine ensures that all scan engines have the same version of virus definitions. This is necessary for proper functioning of virus scanning on the Hitachi Lightning NAS Blade.

You must schedule LiveUpdate on each Symantec AntiVirus Scan Engine. When LiveUpdate is scheduled, LiveUpdate runs at the specified time interval relative to the LiveUpdate base time. The default LiveUpdate base time is the time that the scan engine was installed.

You can change the LiveUpdate base time. If you change the scheduled LiveUpdate interval, the interval adjusts based on the LiveUpdate base time.

For information on changing the base time, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

To schedule LiveUpdate to update virus definitions automatically

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **LiveUpdate**.

2 In the Enable scheduled updates list, select the interval that you want to use.
  This setting is Off by default.

3 Click **Confirm Changes** to save the configuration.

4 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

Configuring the Hitachi Lightning NAS Blade

For each Hitachi Lightning NAS Blade for which you are providing virus scanning, you must register at least one Symantec AntiVirus Scan Engine. You also must configure the virus scan functionality in accordance with the Hitachi documentation. The Hitachi Lightning NAS Blade for which you are providing virus scanning must be in the Lightning 9900V series of network-attached storage devices.

For more information, see the appropriate Hitachi documentation.

Registering the Symantec AntiVirus Scan Engine

For each Hitachi Lightning NAS Blade, you must register at least one Symantec AntiVirus Scan Engine to provide the virus scanning. In a typical environment, a minimum of two scan engines is required to handle scan volume. Four or more (up to 32 total) scan engines are recommended. The NAS Anti Virus Agent handles load balancing across multiple scan engines automatically.

Note: You do not need to register the same scan engine to each Hitachi Lightning NAS Blade within a cluster. You can register different scan engines to different Blades in the same cluster. All of the scan engines that are registered in a cluster must have an identical configuration.

You register the Symantec AntiVirus Scan Engine through the NAS Management interface in the Add Scanner Server window. You must provide the IP address and port number for each scan engine that will be used for scanning. The port number must match the port number that was selected during installation of the Symantec AntiVirus Scan Engine.

Configuring virus scanning on the Hitachi Lightning NAS Blade

You must configure virus scanning (the NAS Anti Virus Agent) for each Hitachi Lightning NAS Blade. You configure the virus scan functionality through the NAS Management interface in the Scan Conditions window for each Blade.

Note: The virus scan functionality for each Hitachi Lightning NAS Blade in a cluster must be configured identically to avoid inconsistency. If the settings for a Blade in a cluster are different, dispersion can occur in the scan results and repair results for infected files.

The virus scan functionality for each Hitachi Lightning NAS Blade should be configured in accordance with the Hitachi documentation and the supplemental guidance in Table 3-2.

Table 3-2 NAS Anti Virus Agent settings

Setting	Description
Scan timing (when to scan files)	Select when files are scanned. You can select from the following: ■ Read and write (recommended): Files are scanned when they are submitted for storage or changed on the NAS device (write) or when they are accessed from storage (read). ■ Read: Files are scanned on read only. ■ Write: Files are scanned on write only.
Extensions for scanning (file types to be scanned)	Select the file types to be passed to the Symantec AntiVirus Scan Engine for scanning. You can use either an exclusion or an inclusion list, or you can scan all files regardless of extension. This setting is identical to the File types to be scanned setting on the Symantec AntiVirus Scan Engine. You must configure this setting on both the Hitachi Lightning NAS Blade and the Symantec AntiVirus Scan Engine. See "Specifying which file types are scanned" on page 37. The recommended setting is to pass all file types to the scan engine except those that are contained in the exclusion list.

Table 3-2 NAS Anti Virus Agent settings

Setting	Description
Maximum file size for scanning	Select whether to specify an upper limit for the size of files to be scanned. If you choose to limit file size, you specify the maximum file size in megabytes. Although you can choose a file size between 1 and 9999 MB, the maximum file size that can be scanned by the Symantec AntiVirus Scan Engine is 2047 MB. The default setting (recommended) is 2047 MB. You can choose to allow or deny access to files that are larger than the limit that is specified in Maximum file size. **Note:** Allowing access to files that have not been scanned for viruses can make your network vulnerable to virus attacks.
Method of dealing with infected files	Specify how unrepairable infected files are handled. The NAS Anti Virus Agent can do any of the following: ■ Delete the file: Deny access to the file, and delete the infected file from storage. If the file has not yet been stored on the Hitachi Lightning NAS Blade, the temporary backup copy of the file is deleted and the file is not stored. ■ Deny access: Deny access to the file, but do not delete the file from storage. ■ Allow access: Allow access to the infected file, and do not delete the file from storage.
Notification when infection is detected	Select whether to receive SNMP notification regarding detection of infected files.
Connection time-out period	Specify the maximum amount of time (in seconds) to wait for a reply from the scan engine when a connection request is sent. A scan engine that does not respond in the specified amount of time is dropped from rotation for a period of time, and the connection request is sent to another scan engine.

Table 3-2 NAS Anti Virus Agent settings

Setting	Description
Scanning time-out period	Specify the maximum amount of time (in seconds) to wait for a scan to finish. If no response is received from the scan engine in the specified amount of time, the procedure that you select for when scanning fails applies. **Note:** To avoid tying up resources, this setting should match the maximum extract time that is specified for container files on the Symantec AntiVirus Scan Engine. The default setting on the Symantec AntiVirus Scan Engine is 180 seconds.
Retry other server count (number of tries to contact the scan engine)	Specify the number of times to request virus scanning for a given file from other registered scan engines that are in the rotation when a connection time-out occurs. This value should equal the number of registered scan engines.
Procedure if scanning fails	Select whether to allow or deny access to a file when virus scanning fails for any reason. **Note:** Allowing access to files that have not been scanned for viruses can make your network vulnerable to virus attacks.
Server monitoring interval	Specify (in seconds) the interval at which registered scan engines are contacted to confirm the status.
Cache size	Specify the size (in megabytes) of the cache that stores information on files that have been previously scanned for viruses.

Known issues with the Hitachi Lightning NAS Blade

The following are known issues with the Hitachi Lightning NAS Blade:

- If you are using multiple scan engines to support scanning, the configuration settings on each Symantec AntiVirus Scan Engine must be identical.
- If you are using multiple scan engines to support scanning, LiveUpdate must be scheduled to occur at the same time on all scan engines so that virus definitions are consistent at all times.

- The virus scan functionality must be configured identically for each Hitachi Lightning NAS Blade in a cluster to avoid inconsistency.
  If the settings for Blades in a cluster are different, dispersion can occur in the scan results and repair results for infected files.
- In the NAS client interface, movements in a directory are interpreted as actions. If you move the cursor over a file name, the file is automatically submitted for scanning. When you change directories, the top-level file in the new directory is submitted for scanning automatically.
  As a result, scanning statistics that are reported on the Status page on the Symantec AntiVirus Scan Engine administrative interface, as well as log entries for infections found (if you have chosen not to delete unrepairable infected files), may reflect multiple scans for the same file.
  Conversely, if you have chosen to delete infected files on the NAS device and a virus is found in a file that was submitted for scanning automatically (due to movements in the directory), the file remains in the directory listing until you refresh the screen even though it has been deleted. You will receive a File not found error message if you try to access that file.

Chapter 4

Configuring Symantec AntiVirus for Sun® StorEdge™ 9900 NAS Blade

This chapter includes the following topics:

- Software components
- How the Symantec AntiVirus Scan Engine works with the Sun StorEdge 9900 NAS Blade
- Preparing for installation
- Configuring the Symantec AntiVirus Scan Engine
- Configuring the Sun StorEdge 9900 NAS Blade
- Known issues with the Sun StorEdge 9900 NAS Blade

Software components

Symantec AntiVirus for Network Attached Storage provides virus scanning and repair capabilities for the Sun® StorEdge™ 9900 series of network-attached storage (NAS) devices.

Adding antivirus scanning to the Sun StorEdge 9900 NAS Blade requires configuration of the following components:

- The Symantec AntiVirus Scan Engine, which provides the virus scanning and repair services
  For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.
- The NAS Anti Virus Agent
  The NAS Anti Virus Agent provides the virus scanning functionality and must be installed and configured on all Sun StorEdge 9900 NAS Blades in a cluster.

How the Symantec AntiVirus Scan Engine works with the Sun StorEdge 9900 NAS Blade

Symantec AntiVirus for Network Attached Storage provides virus scanning and repair capabilities for the Sun StorEdge 9900 series of network-attached storage devices. Virus scanning and repair is provided for files on the Common Internet File System (CIFS).

The Internet Content Adaptation Protocol (ICAP) is used to communicate with the Symantec AntiVirus Scan Engine. In a typical Sun StorEdge 9900 NAS environment, a minimum of two scan engines is required to handle scan volume. Four or more scan engines are recommended. The NAS Anti Virus Agent handles load balancing across multiple scan engines automatically.

How files are scanned

You can configure when the Sun StorEdge 9900 NAS Blade submits files to the Symantec AntiVirus Scan Engine for scanning. You can select from the following:

- Read and write (recommended): Files are scanned when they are submitted for storage or changed on the NAS device (write) or when they are accessed from storage (read).
- Read: Files are scanned on read only.
- Write: Files are scanned on write only.

When a user attempts to access a file from storage, the NAS Anti Virus Agent opens a connection with the Symantec AntiVirus Scan Engine and passes the file to the scan engine for scanning. When scanning is complete, the NAS Anti Virus Agent closes the connection with the scan engine.

After a file is scanned, the Symantec AntiVirus Scan Engine indicates the scanning results to the NAS Anti Virus Agent. If a file is infected and can be repaired, the scan engine also returns the repaired file.

After the NAS Anti Virus Agent receives the scanning results, the file is handled according to the configuration options that are selected. Clean files are passed to the requesting user. If the file is infected and can be repaired, the repaired file is passed to the requesting user, and the stored version of the infected file is replaced with the repaired file. If the file is infected and cannot be repaired, the user is denied access to the file, and the infected file is deleted from storage.

How caching works

The NAS Anti Virus Agent caches scanning results for each clean file. The cached information includes the date and revision number of the virus definitions that were used to perform the scan. In this way, if a second user requests access to a file that has already been scanned and the virus definitions have not changed, a redundant scan is avoided.

The cache is purged when the virus definitions on the Symantec AntiVirus Scan Engine are updated and when the Sun StorEdge 9900 NAS Blade is restarted. Individual cache entries are updated whenever a stored file is changed.

Specifying which file types are scanned

To specify the types of files to be scanned for viruses, you must configure settings on both the NAS Anti Virus Agent and the Symantec AntiVirus Scan Engine.

Specifying file types on the NAS Anti Virus Agent

The NAS Anti Virus Agent makes an initial determination, based on file extension, about whether to pass a file to the Symantec AntiVirus Scan Engine for scanning. You configure which files are passed to the Symantec AntiVirus Scan Engine for scanning when you set up the NAS Anti Virus Agent.

You can control which files are scanned by using either an exclusion or an inclusion list, or you can scan all files regardless of extension. You should configure the NAS Anti Virus Agent to pass all file types to the scan engine except those that are contained in the exclusion list. The default exclusion list is

prepopulated with extensions for those file types that are not likely to contain viruses and can be excluded from scanning. You can customize this list.

See "Configuring virus scanning on the Sun StorEdge 9900 NAS Blade" on page 62.

Specifying file types on the Symantec AntiVirus Scan Engine

The Symantec AntiVirus Scan Engine must be configured to scan selected file types. The scan policy on the Symantec AntiVirus Scan Engine is as important as the NAS Anti Virus Agent setting. It is used after the scan engine receives a file from the NAS Anti Virus Agent to determine which files to scan of those that are contained in archive or container file formats. You can control which embedded files are scanned by using either an exclusion or an inclusion list, or you can scan all files regardless of extension.

Note: Inclusion and exclusion lists do not scan all file types; therefore, new types of viruses might not be detected. Scanning all files regardless of extension is the most secure setting, but it imposes the heaviest demand on resources. During virus outbreaks, you might want to scan all files even if you normally control the file types that are scanned with the inclusion or exclusion list.

For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

See "Specifying which file types to scan on the scan engine" on page 58.

Specifying the scan policy

You configure the scan policy through the Symantec AntiVirus Scan Engine administrative interface. When an infected file is found, the scan engine can do any of the following:

- Scan only: Scan files for viruses, but do nothing to infected files.
- Scan and delete: Scan files for viruses, and delete any infected files that are embedded in archive or container files without attempting repair.
- Scan and repair files: Attempt to repair infected files, but do nothing to unrepairable files (that is, do not delete the files from archive or container files).
- Scan and repair or delete: Attempt to repair infected files, and delete unrepairable files from archive or container files.

Handling of infected files on the NAS device

When an unrepairable infected file is found, the NAS Anti Virus Agent can be configured to do any of the following:

- Delete the file: Deny access to the file, and delete the infected file from storage.
  If the file has not yet been stored on the Sun StorEdge 9900 NAS Blade, the temporary backup copy of the file is deleted, and the file is not stored.
- Deny access: Deny access to the file, but do not delete the file from storage.
- Allow access: Allow access to the infected file, and do not delete the file from storage.

Preparing for installation

Ensure that the computer on which you plan to install the Symantec AntiVirus Scan Engine meets the system requirements that are listed in the *Symantec AntiVirus Scan Engine Implementation Guide*.

After you have installed the Symantec AntiVirus Scan Engine, you must configure the virus scanning functionality on the Sun StorEdge 9900 NAS Blade.

Configuring the Symantec AntiVirus Scan Engine

You must configure several settings on each Symantec AntiVirus Scan Engine that is used to support scanning for the Sun StorEdge 9900 NAS Blade.

Warning: If you are using multiple scan engines to support scanning, the configuration settings on each scan engine must be identical. LiveUpdate should be scheduled to occur at the same time on all scan engines so that virus definitions are consistent at all times.

The scan engine must be configured to use ICAP as the communication protocol. ICAP is the default protocol at installation. After you have selected ICAP, you must configure several ICAP-specific options.

Configuring ICAP-specific options

After you install the Symantec AntiVirus Scan Engine, you can configure several settings that are specific to the ICAP protocol through the Symantec AntiVirus Scan Engine administrative interface. If the Symantec AntiVirus Scan Engine

has already been configured to use another protocol, you also can change the protocol through the administrative interface.

For more information about accessing the administrative interface, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Table 4-1 describes the protocol-specific options for ICAP.

Table 4-1 Protocol-specific options for ICAP

Option	Description
Scan engine bind address	By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by entering the appropriate bind address.
Port number	The port number must be exclusive to the Symantec AntiVirus Scan Engine. For ICAP, the default port number is 1344. If you change the port number, use a number greater than 1024 that is not in use by any other program or service.
HTML message displayed for infected files	This setting is not applicable for the Sun StorEdge 9900 NAS Blade and should be left at the default setting.
ICAP scan policy	When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following: ■ Scan only: Scan files for viruses, but do nothing to infected files. ■ Scan and delete: Scan files for viruses, and delete any infected files that are embedded in archive or container files without attempting repair. ■ Scan and repair files: Attempt to repair infected files, but do nothing to unrepairable files (that is, do not delete the files from archive or container files). ■ Scan and repair or delete: Attempt to repair infected files, and delete unrepairable files from archive or container files.
Data trickle	This setting is not applicable for the Sun StorEdge 9900 NAS Blade. This setting should be left at the default setting (off).

To configure ICAP-specific options

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **ICAP**.
   The configuration settings are displayed for the selected protocol.
   If you change the protocol setting from RPC to ICAP through the Symantec AntiVirus Scan Engine administrative interface, you must manually stop and restart the service (rather than clicking Restart on the administrative interface).
3. Under ICAP Protocol Configuration, in the Scan Engine bind address box, type a bind address, if necessary.
   By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address.
4. In the Port number box, type the TCP/IP port number that the NAS Anti Virus Agent uses to pass files to the Symantec AntiVirus Scan Engine for scanning.
   The default setting for ICAP is port 1344.
5. In the ICAP scan policy list, select how you want the Symantec AntiVirus Scan Engine to handle infected files.
   The default setting is Scan and repair or delete. This is the recommended setting.
6. Click **Confirm Changes** to save the configuration.
7. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the scan engine service now.
     You must stop and restart the service manually if you have changed the communication protocol setting from RPC to ICAP through the administrative interface (rather than selecting ICAP at installation).
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

Specifying which file types to scan on the scan engine

To specify the types of files to be scanned for viruses, you must configure settings on the Symantec AntiVirus Scan Engine. The scan policy on the Symantec AntiVirus Scan Engine is used after the scan engine receives a file from the NAS Anti Virus Agent to determine which files to scan of those that are contained in archive or container file formats.

You can control which embedded files are scanned by using either an exclusion or an inclusion list, or you can scan all files regardless of extension. The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with extensions that are listed in the prepopulated exclusion list.

Note: The Symantec AntiVirus Scan Engine examines the first few bytes of every file to determine whether the file could contain a virus, even if the file extension is not one that was identified for scanning. Based on this examination, the scan engine may scan a file even though it has not been identified for scanning.

For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

See "Configuring virus scanning on the Sun StorEdge 9900 NAS Blade" on page 62.

Specify which file types to scan

You can control which file types are scanned by specifying extensions that you want to include or exclude from scanning, or you can scan all files regardless of extension.

To scan all files except for those that are in the exclusion list

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files except those with the following extensions**.
   This is the recommended setting.
3. Edit the exclusion list to add extensions that you do not want to scan or to delete extensions that you want to scan.
   Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To exclude files with no extension, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.
4. To restore the default extension list, click **Restore default lists**.

5 Click **Confirm Changes** to save the configuration.

6 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

To scan only files that are in the inclusion list

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.

2 On the AntiVirus tab, under File types to be scanned, check **Scan files with the following extensions**.

3 Edit the inclusion list to add extensions that you want to scan or to delete extensions that you do not want to scan.
Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To scan files that have no extensions, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.

4 Click **Confirm Changes** to save the configuration.

5 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

To scan all files regardless of extension

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files regardless of extension**.
3. Click **Confirm Changes** to save the configuration.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the scan engine service now.
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

Scheduling LiveUpdate to update virus definitions automatically

Scheduling LiveUpdate to occur automatically at a specified time interval ensures that the Symantec AntiVirus Scan Engine always has the most current virus definitions. If you are using multiple scan engines to support virus scanning, scheduling LiveUpdate to occur at the same time for each scan engine ensures that all scan engines have the same version of virus definitions. This is necessary for proper functioning of virus scanning on the Sun StorEdge 9900 NAS Blade.

You must schedule LiveUpdate on each Symantec AntiVirus Scan Engine. When LiveUpdate is scheduled, LiveUpdate runs at the specified time interval relative to the LiveUpdate base time. The default LiveUpdate base time is the time that the scan engine was installed.

You can change the LiveUpdate base time. If you change the scheduled LiveUpdate interval, the interval adjusts based on the LiveUpdate base time.

For more information on changing the base time, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

To schedule LiveUpdate to update virus definitions automatically

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **LiveUpdate**.
2. In the Enable scheduled updates list, select the interval that you want to use.
   This setting is Off by default.
3. Click **Confirm Changes** to save the configuration.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the scan engine service now.
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

Configuring the Sun StorEdge 9900 NAS Blade

For each Sun StorEdge 9900 NAS Blade for which you are providing virus scanning, you must register at least one Symantec AntiVirus Scan Engine. You also must configure the virus scan functionality in accordance with the Sun StorEdge documentation. The Sun StorEdge 9900 NAS Blade for which you are providing virus scanning must be in the Lightning 9900 series of network-attached storage devices.

For more information, see the appropriate Sun StorEdge documentation.

Registering the Symantec AntiVirus Scan Engine

For each Sun StorEdge 9900 NAS Blade, you must register at least one Symantec AntiVirus Scan Engine to provide the virus scanning. In a typical environment, a minimum of two scan engines is required to handle scan volume. Four or more (up to 32 total) scan engines are recommended. The NAS Anti Virus Agent handles load balancing across multiple scan engines automatically.

Note: You do not need to register the same scan engine to each Sun StorEdge 9900 NAS Blade within a cluster. You can register different scan engines to different Blades in the same cluster. All of the scan engines that are registered in a cluster must have an identical configuration.

You register the Symantec AntiVirus Scan Engine through the NAS Management interface in the Add Scanner Server window. You must provide the IP address and port number for each scan engine that will be used for scanning. The port number must match the port number that was selected during installation of the Symantec AntiVirus Scan Engine.

Configuring virus scanning on the Sun StorEdge 9900 NAS Blade

You must configure virus scanning (the NAS Anti Virus Agent) for each Sun StorEdge 9900 NAS Blade. You configure the virus scan functionality through the NAS Management interface in the Scan Conditions window for each Blade.

Note: The virus scan functionality for each Sun StorEdge 9900 NAS Blade in a cluster must be configured identically to avoid inconsistency. If the settings for the Blades in a cluster are different, dispersion can occur in the scan results and repair results for infected files.

The virus scan functionality for each Sun StorEdge 9900 NAS Blade should be configured in accordance with the Sun StorEdge documentation and the supplemental guidance in Table 4-2.

Table 4-2 NAS Anti Virus Agent settings

Setting	Description
Scan timing (when to scan files)	Select when files are scanned. You can select from the following: ■ Read and write (recommended): Files are scanned when they are submitted for storage or changed on the NAS device (write) or when they are accessed from storage (read). ■ Read: Files are scanned on read only. ■ Write: Files are scanned on write only.

Table 4-2 NAS Anti Virus Agent settings

Setting	Description
Extensions for scanning (file types to be scanned)	Select the file types to be passed to the Symantec AntiVirus Scan Engine for scanning. You can use either an exclusion or an inclusion list, or you can scan all files regardless of extension. This setting is identical to the File types to be scanned setting on the Symantec AntiVirus Scan Engine. You must configure this setting on both the Sun StorEdge 9900 NAS Blade and the Symantec AntiVirus Scan Engine. See "Specifying which file types are scanned" on page 53. The recommended setting is to pass all file types to the scan engine except those that are contained in the exclusion list.
Maximum file size for scanning	Select whether to specify an upper limit for the size of files to be scanned. If you choose to limit file size, you specify the maximum file size in megabytes. Although you can choose a file size between 1 and 9999 MB, the maximum file size that can be scanned by the Symantec AntiVirus Scan Engine is 2047 MB. The default setting (recommended) is 2047 MB. You can choose to allow or deny access to files that are larger than the limit that is specified in Maximum file size. **Note:** Allowing access to files that have not been scanned for viruses can make your network vulnerable to virus attacks.
Method of dealing with infected files	Specify how unrepairable infected files are handled. The NAS Anti Virus Agent can do any of the following: ■ Delete the file: Deny access to the file, and delete the infected file from storage. If the file has not yet been stored on the Sun StorEdge 9900 NAS Blade, the temporary backup copy of the file is deleted and the file is not stored. ■ Deny access: Deny access to the file, but do not delete the file from storage. ■ Allow access: Allow access to the infected file, and do not delete the file from storage.
Notification when infection is detected	Select whether to receive SNMP notification regarding detection of infected files.

Table 4-2 NAS Anti Virus Agent settings

Setting	Description
Connection time-out period	Specify the maximum amount of time (in seconds) to wait for a reply from the scan engine when a connection request is sent. A scan engine that does not respond in the specified amount of time is dropped from rotation for a period of time, and the connection request is sent to another scan engine.
Scanning time-out period	Specify the maximum amount of time (in seconds) to wait for a scan to finish. If no response is received from the scan engine in the specified amount of time, the procedure that you select for when scanning fails applies. **Note:** To avoid tying up resources, this setting should match the maximum extract time that is specified for container files on the Symantec AntiVirus Scan Engine. The default setting on the Symantec AntiVirus Scan Engine is 180 seconds.
Retry other server count (number of tries to contact the scan engine)	Specify the number of times to request virus scanning for a given file from other registered scan engines that are in the rotation when a connection time-out occurs. This value should equal the number of registered scan engines.
Procedure if scanning fails	Select whether to allow or deny access to a file when virus scanning fails for any reason. **Note:** Allowing access to files that have not been scanned for viruses can make your network vulnerable to virus attacks.
Server monitoring interval	Specify (in seconds) the interval at which registered scan engines are contacted to confirm the status.
Cache size	Specify the size (in megabytes) of the cache that stores information on files that have been previously scanned for viruses.

Known issues with the Sun StorEdge 9900 NAS Blade

The following are known issues with the Sun StorEdge 9900 NAS Blade:

- If you are using multiple scan engines to support scanning, the configuration settings on each Symantec AntiVirus Scan Engine must be identical.
- If you are using multiple scan engines to support scanning, LiveUpdate must be scheduled to occur at the same time on all scan engines so that virus definitions are consistent at all times.
- The virus scan functionality must be configured identically for each Sun StorEdge 9900 NAS Blade in a cluster to avoid inconsistency.
  If the settings for Blades in a cluster are different, dispersion can occur in the scan results and repair results for infected files.
- In the Sun StorEdge 9900 NAS client interface, movements in a directory are interpreted as actions. If you move the cursor over a file name, the file is automatically submitted for scanning. When you change directories, the top-level file in the new directory is submitted for scanning automatically.
  As a result, scanning statistics that are reported on the Status page on the Symantec AntiVirus Scan Engine administrative interface, as well as log entries for infections found (if you have chosen not to delete unrepairable infected files), may reflect multiple scans for the same file.
  Conversely, if you have chosen to delete infected files on the storage device and a virus is found in a file that was submitted for scanning automatically (due to movements in the directory), the file remains in the directory listing until you refresh the screen even though it has been deleted. You will receive a File not found error message if you try to access that file.

Index

A

antivirus scanning 15

F

file types to be scanned
- Hitachi Lightning NAS Blade 41
- NetApp Filer 28
- Sun StorEdge 9900 NAS Blade 58

H

Hitachi Lightning NAS Blade
- configuring for virus scanning 45
- configuring scan engine 39
- known issues 48
- overview of virus scanning 36
- software components 35
- specifying files to scan 41
- system requirements 36

N

NetApp Filer
- configuring for virus scanning 31
- configuring scan engine 22
- editing service startup properties 28
- known issues 32
- logging of scan engine events 20
- overview of virus scanning 18
- quarantining infected files 26
- software components 17
- specifying files to scan 28
- system requirements 21
- user notification of infection found 21, 26

notification of infection found, NetApp Filer 21, 26

Q

quarantining infected files, NetApp Filer 26

S

service startup properties, NetApp Filer 28
software components
- Hitachi Lightning NAS Blade 35
- NetApp Filer 17

Sun StorEdge 9900 NAS Blade
- configuring for virus scanning 61
- configuring scan engine 55
- known issues 65
- overview of virus scanning 52
- specifying files to scan 58
- system requirements 52

Symantec AntiVirus for Network Attached Storage
- documentation 12
- software components 12
- supported devices 12

Symantec AntiVirus Scan Engine
- configuring for Hitachi Lightning NAS Blade 39
- configuring for NetApp Filer 22
- configuring for Sun StorEdge 9900 NAS Blade 55
- documentation 13
- virus protection 15

V

virus protection
- description 15
- for network attached storage 14